UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/615,829	07/10/2003	Franck Le	088245-0111	8920

23524 7590 11/01/2007

FOLEY & LARDNER LLP
150 EAST GILMAN STREET
P.O. BOX 1497
MADISON, WI 53701-1497

EXAMINER	
KLIMACH, PAULA W	

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
11/01/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/615,829	LE ET AL.	
	Examiner	Art Unit	
	Paula W. Klimach	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 August 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *29-89* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *29-89* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 08/20/07 has been entered.

Response to Arguments

Applicant's arguments filed 08/20/07 have been fully considered.

The applicant argued that Montenegro states that the public key is the DSA public key. Montenegro fails to teach, suggest, or disclose calculating a first address value based on the identified secret value and the identified number of identification allowed. This is not found persuasive. Montenegro teaches the public key as disclosed by the applicant. This public key has a private key pair and therefore the public key is based on the public key and it thus follows that the address of Montenegro is based on the private key pair that is dependent on the public key. Furthermore, the newly cited art teaches the identification allowed.

The applicant argued further that Montenegro fails to teach, suggest, or disclose "calculating a plurality of random values using the identified plurality of random bits and the identified plurality of random integers. The newly cited art teaches the missing limitation.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 29-65 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. The claims recite "...identifying a number of identifications allowed," further the number of identifications allowed is used to calculate a first address. However, in the specification there is no mention of identifying a number of identification allowed. Furthermore there is no mention of using the value to calculate the first address.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 29-65 are rejected under 35 U.S.C. 103(a) as being unpatentable over Montenegro et al ("Statistically Unique and Cryptographically Verifiable (SUCV) identifiers and addresses") in view of Watson et la (5,475,839) in view of Henry (6,971,005).

In reference to claims 29, 42, 48, 60 Montenegro discloses a method of addressing the identifier ownership problem by using characteristics of Statistic Uniqueness and Cryptographic Verifiability wherein the SUCV addresses can solve the address ownership problem (Introduction). The system of Montenegro includes identifying a secret value (private key) at a first device (Section 4), the public key system contains a public key and private key pair; calculating a first address value based on the identified secret value (Section 5.3); generating an address as a concatenation of a second address value and the calculated first address value (Section 5.2); sending the generated address from the first device to a second device (sucvP3 section 6.2); receiving a request to confirm ownership of the generated address from the second device at the first device (sucvP1 section 6.2); calculating a first value based on the identified secret value and the identified number of confirmations performed (section 6.2); and sending a first message from the first device to the second device, the first message including the calculated first value so that the second device can confirm ownership of the generated address by the first device (section 6.2 when CN receives the sucvP3 and verifies the signature).

Watson teaches a method of securing access to a computer (title). The system includes identifying a number of identifications allowed (Fig. 5).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to identify the number of identifications (logins) allowed as in Watson in the system of Montenegro. One of ordinary skill in the art would have been motivated to do this because it limits the ability of a fraudulent user to discover the secret information.

Henry teaches calculating a first address value based on the identified number of identifications allowed; identifying a number of confirmations previously performed between the

first device and the second device (column 3 lines 45-50). Since the values can only be calculated after a successful logon and therefore the first address is a value based on the number of times the user is allowed to identify themselves.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to identify the number of identifications (logins) allowed as in Henry in the system of Montenegro. One of ordinary skill in the art would have been motivated to do this because it limits the ability of a fraudulent user to discover the secret information.

In reference to claim 30, 37, 43, 53, 65 the system of Montenegro further comprising receiving a router advertisement message including an address prefix, wherein the second address value comprises the address prefix (Section 5.2).

In reference to claim 31, 38, 44 Montenegro discloses further comprising repeating (f), (g), (h), (i) (last paragraph section 6.2).

In reference to claim 32, 39, 45 Montenegro does not disclose a system wherein the first message further includes the identified number of confirmations performed.

Watson teaches a method of securing access to a computer (title). The system includes identifying a number of identifications allowed (Fig. 5). This allows the system to try to send a message further including the identified number of confirmations performed.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to identify the number of identifications (logins) allowed as in Watson in the system of Montenegro. One of ordinary skill in the art would have been motivated to do this because it limits the ability of a fraudulent user to discover the secret information.

In reference to claim 33, 40, 46 Montenegro does not teach comparing the identified number of confirmations performed with the defined number of identifications allowed; and based on an outcome of the comparison, identifying a second secret value at the first device.

Watson teaches a method of securing access to a computer (title). The system includes identifying a number of identifications allowed and comparing the identified number of confirmations performed with the defined number of identifications allowed (Fig. 5). This allows the system to try to and based on an outcome of the comparison, identifying a second secret value at the first device.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to identify the number of identifications (logins) allowed as in Watson in the system of Montenegro. One of ordinary skill in the art would have been motivated to do this because it limits the ability of a fraudulent user to discover the secret information.

In reference to claim 34 Montenegro teaches further comprising repeating (c)-(i) replacing the identified secret value with the identified second secret value (section 6.4).

In reference to claim 35, 41, 47, 52, 64 Montenegro teaches a system wherein the first message comprises a binding update message sent using a mobile Internet protocol version 6 protocol (section 6.2).

In reference to claim 36 and 54 the claim is rejected as in claim 1 above and the system further comprises a processor; a communication interface operably coupled to the processor (Montenegro section 6 and section 7).

In reference to claims 49, 55, 61 further comprising updating the second number of confirmations performed at the second device.

Watson teaches a method of securing access to a computer (title). The system includes identifying a number of identifications allowed (Fig. 5). Updating the second number of confirmations performed at the second device takes place in parts 3, 5, 7, and 9 in Fig. 5

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to identify the number of identifications (logins) allowed as in Watson in the system of Montenegro. One of ordinary skill in the art would have been motivated to do this because it limits the ability of a fraudulent user to discover the secret information.

In reference to claims 50, 56, 62 Montenegro discloses a system wherein comparing the calculated first value with the value maintained at the second device comprising calculating a second value by applying a hash function to the calculated first value (section 7); and comparing the calculated second value with the value maintained at the second device (section 7).

In reference to claims 51, 57, 63 Montenegro teaches a system further comprising after storing the calculated second value at the second device as the value maintained at the second device (Section 7).

Claims 66, 71, 76, 81, 84-85, and 87-88 are rejected under 35 U.S.C. 103(a) as being unpatentable over Montenegro in view of the book by Schneier (Applied Cryptography).

In reference to claims 66, 76, 81, 84, 87 Montenegro discloses a method of addressing the identifier ownership problem by using characteristics of Statistic Uniqueness and Cryptographic Verifiability wherein the SUCV addresses can solve the address ownership problem (Introduction). The system of Montenegro includes identifying a plurality of random integers, (Section 4); identifying a plurality of random bits associated with the plurality of

random integers (Section 5.3); calculating a plurality of random values using the identified plurality of random bits and the identified plurality of random integers, public and private keys (Section 5.3); calculating a first address value based on the calculated plurality of random values, sucvHID (Section 5.2); generating an address as a concatenation of a second address value and the calculated first address value (section 7); calculating a first value based on a first random integer (section 7); providing the generated address and the calculated first value to a second device (section 8.2.2); receiving a request to confirm ownership of the generated address from the second device at a first device, the request including a plurality of bit values (sucvP2 Section 6.2); calculating a second value based on the received plurality of bit values, and the identified plurality of random integers (section 6.2); and sending a first message from the first device to the second device, the first message including the calculated second value, the calculated plurality of random values, so that the second device can confirm ownership of the generated address by the first device (section 6.2).

Montenegro does not teach identifying a plurality of random integers, wherein the plurality of random integers are less than a defined maximum value.

Schneier discloses random pseudo-random-sequence generation and thus identifying a plurality of random integers, wherein the plurality of random integers are less than a defined maximum value, in the form of a pseudo-random sequence (page 44-45). The maximum value occurs when the sequence is long enough so that a finite sequence of reasonable length tha is one that is not periodic.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize the random sequence is taught by Schneier in the system of Montenegro.

One of ordinary skill in the art would have been motivated to do this because it reduces the ability of a cryptanalyst to attack a system.

In reference to claim 71 the claim is rejected as in claim 1 above and the system further comprises a processor; a communication interface operably coupled to the processor (Montenegro section 6 and section 7).

In reference to claims 85, 88 Montenegro discloses a system wherein comparing the calculated first value with the value maintained at the second device comprising calculating a second value by applying a hash function to the calculated first value (section 7); and comparing the calculated second value with the value maintained at the second device (section 7).

Claims 67-70, 72-75, 77-80, 82-83, 86, and 89 are rejected under 35 U.S.C. 103(a) as being unpatentable over Montenegro in view of Schneier as applied to claims *66, 71, 76, 81, 84, 87* above, and further in view of Thomlinson (5,778,069).

In reference to claims 67, 72, 77, 82 Montenegro does not discloses a system wherein calculating the first address value comprises applying a hash function to the calculated plurality of random values.

Thomlinson discloses a pseudo random number generator wherein calculating the first address value comprises applying a hash function to the calculated plurality of random values (Fig. 3).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize the method of Thomlinson to generate a random number using a hash function in the system of Montenegro. One of ordinary skill in the art would have been

motivated to do this because the hash function would make it impossible to determine the input value and therefore discourage fraud.

In reference to claims 68, 73, 78 Montenegro does not disclose a system wherein calculating the plurality of random values comprises solving the equation $vi = (-1)^{b}_{i}.(s_i^2)^{-1} \bmod n$ for $1<i<k$, where vi is the plurality of random values, b_i, is the plurality of random bits, s_i is the plurality of random integers, n is the defined maximum value, and k is a security parameter.

Thomlinson discloses a pseudo random number generator wherein calculating the first address value comprises applying a hash function to the calculated plurality of random values (Fig. 3). The hash function performs the function of the equation $vi = (-1)^{b}_{i}.(s_i^2)^{-1} \bmod n$

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize the method of Thomlinson to generate a random number using a hash function in the system of Montenegro. One of ordinary skill in the art would have been motivated to do this because the hash function would make it impossible to determine the input value and therefore discourage fraud.

In reference to claims 69, 74, 79 Montenegro does not disclose a system wherein calculating the first value comprises solving the equation $x = (-1)^{b}.(r^2) \bmod n$, where x is the first value, b is a random bit, and r is the first random integer, and n is the defined maximum value.

Thomlinson discloses a pseudo random number generator wherein calculating the first address value comprises applying a hash function to the calculated plurality of random values (Fig. 3). The hash function performs the function of the equation $x = (-1)^{b}.(r^2) \bmod n$

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize the method of Thomlinson to generate a random number using a hash

function in the system of Montenegro. One of ordinary skill in the art would have been motivated to do this because the hash function would make it impossible to determine the input value and therefore discourage fraud.

In reference to claims 70; 75, 80, 83, 86, 89 wherein calculating the second value comprises solving the equation $y= r*\Pi e_j\ s_j \bmod n$ for $1<j<k$, where y is the second value, r is the first random integer, e_j is the received plurality of bit values, s_j is the plurality of random integers, and n is the defined maximum value.

Thomlinson discloses a pseudo random number generator wherein calculating the first address value comprises applying a hash function to the calculated plurality of random values (Fig. 3). The hash function performs the function of the equation $y= r*\Pi e_j\ s_j$

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize the method of Thomlinson to generate a random number using a hash function in the system of Montenegro. One of ordinary skill in the art would have been motivated to do this because the hash function would make it impossible to determine the input value and therefore discourage fraud.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W. Klimach whose telephone number is (571) 272-3854. The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

PWK
Monday, October 29, 2007

KIM VU
SUPERVISORY PATENT EXAM
TECHNOLOGY CENTER 21